

EXHIBIT 3

Chrome Enterprise Premium documentation

View all product documentation (<https://cloud.google.com/beyondcorp-enterprise/docs/overview>)

Chrome Enterprise Premium is Google Cloud's zero-trust solution that enables an organization's workforce to access web applications securely from anywhere, without the need for VPN and without fear of malware, phishing, and data loss.

By using Chrome Enterprise Premium, you can manage access for apps on Google Cloud, other clouds, and on-premises, define and enforce access policies based on user, device, and other contextual factors, and make apps more accessible and responsive through Google's global network.

Keep exploring with 20+ always-free products

Access 20+ free products for common use cases, including AI APIs, VMs, data warehouses, and more.

View free product offers (</free/docs/free-cloud-features#free-tier-usage-limits>)

Documentation resources

Find quickstarts and guides, review key references, and get help with common issues.



Guides

[Quickstart: Apply Chrome Enterprise Premium to cloud resources](#)

(/beyondcorp-enterprise/docs/apply-resources)

[Overview](#)

(/beyondcorp-enterprise/docs/overview)

[Secure the Google Cloud console and APIs](#)

(/beyondcorp-enterprise/docs/securing-console-and-apis)



Reference

[Audit logging](#)

(/beyondcorp-enterprise/docs/audit-logs)

[Using hostname and path conditions](#)

(/beyondcorp-enterprise/docs/hostname-and-path-conditions)



Resources

[Pricing](#)

(/beyondcorp-enterprise/pricing)

[Release notes](#)

(/beyondcorp-enterprise/docs/release-notes)

[Support](#)

(/beyondcorp-enterprise/docs/support)

[Billing questions](#)

(/beyondcorp-enterprise/docs/billing-questions)

[Securing on-premises apps and resources with IAP](#)

(/beyondcorp-enterprise/docs/securing-on-premises)

[Securing App Engine apps with IAP](#)

(/beyondcorp-enterprise/docs/securing-app-engine)

[Securing non-Google Cloud applications using the app connector](#)

(/beyondcorp-enterprise/docs/enable-app-connector)

Related resources

Explore self-paced training from Google Cloud Skills Boost, use cases, reference architectures, and code samples with examples of how to use and connect Google Cloud services.

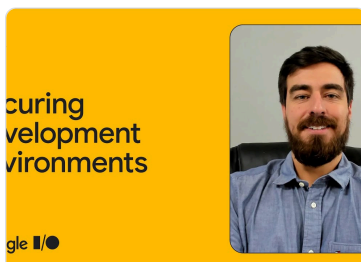
TRAINING

Security in Google Cloud

In this training course, you will learn about a variety of Google Cloud security controls and techniques. You'll explore the components of Google Cloud and deploy a secure solution on the platform. You'll also learn how to mitigate attacks at several points in a Google Cloud-based infrastructure, including distributed denial-of-service attacks, phishing attacks, and threats involving content classification and use.

Learn more [\(/training/course/security-in-google-cloud-platform\)](/training/course/security-in-google-cloud-platform)

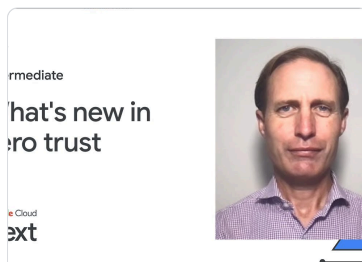
Related videos



YOUTUBE

Securing development environments with Google Cloud

(<https://www.youtube.com/watch?v=hVTnW-rH5Vc>)



YOUTUBE

What's new in zero trust

(<https://www.youtube.com/watch?v=KaeL0C39jDQ>)



YOUTUBE

Google Cloud Security Summit

(<https://www.youtube.com/watch?v=3kMKKaVGQZk>)

Software supply chain security starts where code is created, in the development environments/IDEs. Learn ho...

Google pioneered zero trust for corporate applications with its BeyondCorp approach, and then combined it with in...

The Google Cloud Security Summit brought together leading Google and partner professionals to present the...

[More](#) ▾

Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0) (<https://www.apache.org/licenses/LICENSE-2.0>). For details, see the [Google Developers Site Policies](https://developers.google.com/site-policies) (<https://developers.google.com/site-policies>). Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2025-01-09 UTC.